Claims

We claim:

1. A method for automatically authenticating a user of a first networked application to a second networked application, the method comprising:

the first networked application receiving authentication information from the user;

the first networked application authenticating the user to use the first networked application in response to said receiving the authentication information from the user;

launching the second networked application, wherein said launching comprises the first networked application providing authentication information associated with the user to the second networked application;

the second networked application authenticating the user to use the second networked application in response to receiving said authentication information from the first networked application.

2. The method of claim 1, wherein said launching the second networked application comprises the user performing an action which triggers a programmatic event, the method further comprising:

the first networked application intercepting the event;

the first networked application providing authentication information associated with the user to the second networked application, in response to said first networked application intercepting the event.

3. The method of claim 2,

wherein said launching the second networked application comprises the user clicking on a hypertext link associated with the second application;

wherein said user clicking on the hypertext link triggers a programmatic event representing the click;

wherein the first networked application includes an event handler which intercepts the click event.

4. The method of claim 3,

wherein the event handler is a Javascript event handler.

5. The method of claim 1

wherein said first networked application providing authentication information associated with the user to the second networked application comprises:

the client side of the first networked application requesting and receiving authentication parameters from the server side of the first networked application, wherein the authentication parameters comprise information for authenticating the user to the second networked application;

the client side of the first networked application providing the authentication parameters to the server side of the second networked application.

6. The method of claim 5,

wherein said launching the second networked application comprises the user clicking on a hypertext link associated with the second application;

wherein the first application includes an event handler that intercepts an event triggered by the user clicking on the hypertext link;

wherein the event handler requests and receives authentication parameters from the server side of the first application, wherein the authentication parameters comprise information for authenticating the user to the second networked application;

wherein the event handler passes the authentication parameters to the server side of the second networked application.

7. The method of claim 6,

wherein said event handler passing the authentication parameters to the server side of the second networked application comprises the event handler appending the authentication parameters onto a URL associated with the second networked application;

wherein the event handler performs an HTTP GET request using the resulting URL.

8. The method of claim 6,

wherein said event handler passing the authentication parameters to the server side of the second networked application comprises the event handler performing an HTTP POST request using a URL associated with the second application;

wherein the authentication parameters are sent to the server side of the second networked application as posted data.

9. The method of claim 5,

wherein the server side of the first networked application stores information associated with the user in a database;

wherein the stored user information is used to generate the authentication parameters.

10. The method of claim 9, wherein the user information stored by the server side of the first networked application was previously set by an administrator of the second networked application using an administrative tool.

11. The method of claim 5,

wherein the authentication parameters received from the server side of the first networked application are encrypted.

12. The method of claim 11,

wherein the server side of the first networked application is enabled to apply various cryptographic techniques to the authentication parameters;

wherein an administrator may specify which techniques to apply using an administrative tool.

13. The method of claim 11,

wherein the authentication parameters include a sequence number.

14. The method of claim 11,

wherein the authentication parameters include an expiry time.

16. The method of claim 1, further comprising:

the second networked application launching after said second networked application authenticating the user to use the second networked application.

17. The method of claim 16,

wherein the second networked application is a web application;

wherein said second networked application launching comprises the server side of the second networked application returning an initial web page to the client side of the second networked application.

18. A system for performing single sign-on user authentication, the system comprising:

a first computer system running client-side software associated with a first networked application;

a second computer system connected to the first computer system via a network, wherein server-side software associated with the first networked application runs on the second computer system;

a third computer system connected to the first computer system via a network, wherein server-side software associated with a second networked application runs on the third computer system;

wherein the client-side software associated with the first networked application is operable to:

receive authentication information from a user;

communicate with the server-side software associated with the first networked application in order to authenticate the user to use the first networked application, in response to said receiving the authentication information from the user;

launch the second networked application, wherein said launching comprises providing authentication information associated with the user to the server-side software associated with the second networked application;

wherein the server-side software associated with the second networked application is operable to authenticate the user to use the second networked application, in response to receiving said authentication information from the client-side software associated with the first networked application.

19. The system of claim 18,

wherein said launching the second networked application is performed in response to intercepting a programmatic event triggered by the user requesting to launch the second networked application.

20. The system of claim 18,

wherein said launching the second networked application is performed in response to intercepting a programmatic event triggered by the user clicking on a hypertext link associated with the second application;

wherein the client-side software associated with the first networked application includes an event handler which intercepts the click event.

21. The system of claim 20,

wherein the event handler is a Javascript event handler.

22. The system of claim 18,

wherein said providing authentication information associated with the user to the server-side software associated with the second networked application comprises:

requesting and receiving authentication parameters from the server-side software associated with the first networked application, wherein the authentication parameters comprise information for authenticating the user to the second networked application;

providing the authentication parameters to the server-side software associated with the second networked application.

23. The system of claim 22,

wherein said launching the second networked application is performed in response to the user clicking on a hypertext link associated with the second application;

wherein the client-side software associated with the first networked application includes an event handler that intercepts an event triggered by the user clicking on the hypertext link;

wherein the event handler requests and receives authentication parameters from the server-side software associated with the first networked application, wherein the authentication parameters comprise information for authenticating the user to the second networked application;

wherein the event handler passes the authentication parameters to the server-side software associated with the second networked application.

24. The system of claim 23,

wherein said event handler passing the authentication parameters to the server-side software associated with the second networked application comprises the event

handler appending the authentication parameters onto a URL associated with the second networked application;

wherein the event handler performs an HTTP GET request using the resulting URL.

25. The system of claim 23,

wherein said event handler passing the authentication parameters to the server-side software associated with the second networked application comprises the event handler performing an HTTP POST request using a URL associated with the second networked application;

wherein the authentication parameters are sent to the server-side software associated with the second networked application as posted data.

26. The system of claim 22,

wherein the server-side software associated with the first networked application stores information associated with the user in a database;

wherein the stored user information is used to generate the authentication parameters.

27. The system of claim 26, wherein the user information stored by the server-side software associated with the first networked application was previously set by an administrator of the second networked application using an administrative tool.

28. The system of claim 22,

wherein the authentication parameters received from the server-side software associated with the first networked application are encrypted.

29. The system of claim 28,

wherein the server-side software associated with the first networked application is enabled to apply various cryptographic techniques to the authentication parameters;

wherein an administrator may specify which techniques to apply using an administrative tool.

30. The system of claim 18,

wherein the client-side software associated with the first networked application comprises an application including web-browsing functionality.